The 8 Questions Your Pentest Report Must Answer

A stakeholder guide to getting real value from security assessments

INTRODUCTION

HOW TO USE THIS DOCUMENT

This blueprint outlines the essential elements every penetration test report should include. Each section corresponds to a required component of a high-quality pentest report. Use these 8 questions as a checklist when reviewing reports. If any are missing clear, specific answers, you are not getting full value from your security investment.

THE PROBLEM

Most penetration test reports fail to answer the questions stakeholders actually need answered. Executives get buried in technical jargon. Developers receive generic advice. Auditors struggle to map findings to compliance requirements.

THE SOLUTION

A quality pentest report must answer 8 critical questions, organized by who needs the answer:

- → **Executives and business leaders** need answers to questions 1-3
- → **Technical teams and developers** need answers to questions 4-6
- → **Auditors and compliance officers** need answers to questions 7-8

Who Should Read What

Executives/Board Members: Turn to Page 2
Developers/Security Engineers: Turn to Page 3
Compliance/Audit Teams: Turn to Page 4

WHAT MAKES A GOOD PENTEST REPORT

- → **Answers all 8 questions** with specific, actionable information
- → **Speaks to each audience** in their language
- → **Proves value through validation** showing what was fixed

FOR EXECUTIVES & BUSINESS LEADERS

Strategic Security Questions

The business-critical questions that drive resource allocation, board reporting, and risk management decisions. These should be easy to locate within the first four pages of any quality report.

1 How secure are we?

- Overall risk rating (Critical/High/Medium/Low/Minimal)
- Visual dashboard showing risk distribution
- Identified strengths and effective controls

WHY THIS MATTERS

- ✓ **Executive decision-making:** Board reporting, insurance premiums, M&A due diligence
- ✓ **Resource allocation:** Justify budget increases or prove current investments work
- ✓ **Positive reinforcement:** Knowing what works helps maintain and expand controls

2 What needs to be fixed immediately?

- Prioritized findings ranked by business risk
- Business impact if exploited
- Prioritized action items

WHY THIS MATTERS

- ✓ **Limited resources:** Cannot fix everything at once—focus on highest business risk
- ✓ **Urgency justification:** Explain to stakeholders why this cannot wait until next quarter
- ✓ **Quick wins:** Demonstrate security improvement in weeks, not months

3 Did our remediation efforts work?

- What was fixed vs. what is still broken
- Before-and-after risk posture comparison

WHY THIS MATTERS

- ✓ **Prove ROI:** Validate that security spending actually improved posture
- ✓ **Audit/compliance evidence:** Show auditors you are closing gaps, not just finding them
- ✓ **Continuous improvement:** Track progress over multiple assessment cycles

FOR TECHNICAL & SECURITY TEAMS

Implementation & Remediation Questions

The technical details developers and security engineers need to understand, reproduce, and fix vulnerabilities.

4 What exactly is vulnerable?

- Specific systems, applications, configurations affected
- CVSS or DREAD scoring showing severity and exploitability
- How findings map to industry standards (CWE, CVE, OWASP Top 10)

WHY THIS MATTERS

- ✓ **Precision targeting:** Technical teams need exact locations to fix, not vague descriptions
- ✓ **Standardized comparison:** CVSS scores enable apples-to-apples risk comparison
- ✓ **Compliance mapping:** Prove coverage of OWASP Top 10, PCI-DSS requirements, etc.

5 How would an attacker exploit this?

- Step-by-step reproduction instructions
- Proof-of-concept demonstrations
- Screenshots and technical evidence

WHY THIS MATTERS

- ✓ **Developer understanding:** Engineers need to see the actual threat to write proper fixes
- ✓ **Eliminate skepticism:** Arguments disappear with PoC
- ✓ **Urgency justification:** Showing exploitation makes abstract risks concrete

6 How do we fix it?

- Specific remediation guidance focused on configuration and architectural corrections
- Guidance written in a way that engineers can act on immediately

WHY THIS MATTERS

- ✓ **Accelerate remediation:** Developers do not waste time researching solutions
- ✓ **Reduce consultant dependency:** Teams can fix issues without ongoing support
- ✓ **Quality over speed:** Specific guidance prevents Band-Aid fixes that fail retests

FOR AUDIT & COMPLIANCE TEAMS

Validation & Compliance Questions

The verification and credentialing information auditors and compliance officers need to validate the assessment.

7 What did you actually test?

- Methodology and standards used (OWASP, PTES, etc.)
- Scope: what was included vs. excluded
- Tools and techniques employed
- Time constraints and limitations

WHY THIS MATTERS

- ✓ **Auditor requirements:** Compliance frameworks demand documented methodology
- ✓ **Reveal coverage gaps:** Knowing what was not tested helps plan future assessments
- ✓ **Legal protection:** Clear scope prevents liability disputes
- ✓ **Repeatable process:** Future testers can replicate or expand on the approach

8 Who performed the test and are they qualified?

- Identify who performed the assessment(s), including their role and direct responsibility
- List relevant, performance-based certifications (OSCP, GPEN, GWAPT, or equivalent)
- Document years of practical penetration testing experience

WHY THIS MATTERS

- ✓ **Credibility validation:** Certified professionals carry more weight with auditors
- ✓ **Compliance requirements:** PCI-DSS, HIPAA, SOC 2 often require documented quals
- ✓ **Justify cost:** Stakeholders need to know they are paying for expertise
- ✓ **Legal/insurance:** Documented competency matters for insurance claims and litigation

NEXT STEPS

Use this blueprint to evaluate any penetration test report you receive. If a report fails to answer all eight questions clearly and specifically, it does not meet modern security, engineering, or compliance expectations. Turn to the Report Quality Checklist on Page 5 to score your next report.

REPORT QUALITY CHECKLIST

Does Your Report Make the Cut?

When evaluating your next penetration test report, verify it answers all 8 questions below. If any box remains unchecked, you should be asking your vendor one simple question: **why not?**

- [ ] **Question 1:** Overall risk rating with visual dashboard and identified strengths
- [ ] **Question 2:** Prioritized findings ranked by business risk with impact assessment
- [ ] **Question 3:** Remediation validation with before-and-after risk posture comparison
- [ ] **Question 4:** Specific vulnerable systems with CVSS scores and CWE/CVE mapping
- [ ] **Question 5:** Step-by-step exploitation with PoC demonstrations
- [ ] **Question 6:** Actionable remediation for configuration and architecture
- [ ] **Question 7:** Documented methodology, scope, tools, and limitations
- [ ] **Question 8:** Tester qualifications with certifications and experience

No Fillers. Just Findings.

Voke Cyber delivers penetration testing that checks every box—with retesting included.

vokecyber.com · info@vokecyber.com · (765) 422-5464